



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/921,265	08/01/2001	Warwick Ford	21190-05339	8690
758	7590	07/28/2005		
FENWICK & WEST LLP SILICON VALLEY CENTER 801 CALIFORNIA STREET MOUNTAIN VIEW, CA 94041			EXAMINER HENNING, MATTHEW T	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 07/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/921,265

Applicant(s)

FORD, WARWICK

Examiner

Matthew T. Henning

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 May 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-8 and 10-19 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-8 and 10-19 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 8/1/2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

1 This action is in response to the communication filed on 5/16/2005.

2 **DETAILED ACTION**

3 Claims 1-8, and 10-19 have been examined and claim 9 has been cancelled.

4 All objections and rejections not set forth below have been withdrawn.

5 ***Response to Arguments***

6 Applicant's arguments filed 5/16/2005 have been fully considered but they are not
7 persuasive. Applicant argues primarily that:

8 a. The combination of Fielder and Menezes, as relied upon in the office action dated
9 2/11/2005, is not possible because the combination would destroy the principle of operation of
10 Fielder.

11 Applicant's argument that the combination of Fielder and Menezes would destroy the
12 principle of operation of Fielder has been considered and is not persuasive. Applicant has
13 misinterpreted the principle of operation of Fielder to be not sending the update data from one
14 device to another. However, this is not the case. The principle of operation of Fielder is clearly
15 expressed in the first five lines of the abstract as being "a bilateral system for authenticating
16 remote transceiving stations through use of station identifiers (Ids), and through use of passwords
17 which are used only one time, and thereafter exchanging messages through use of an encryption
18 key which is changed after each system connection." This clearly does not limit the principle of
19 operation of Fielder to not sending the update data between two devices. Fielder has merely
20 expressed that it was preferred that the update data was not sent between the two devices. As
21 such, exchanging the update data does not destroy the principle of operation. More specifically,
22 it does not stop the system from authenticating remote transceiving stations through use of

Art Unit: 2131

1 station identifiers, and through use of one-time passwords. Nor does it prevent the system from
2 exchanging messages through use of an encryption key which is changed after each system
3 connection. Instead, the combination merely changes the way the key is updated, which does not
4 destroy the principle of operation. Furthermore, Menezes has provided clear motivation for
5 having the server generate this data randomly and exchanging this data between the server and
6 the client on Page 398 Section (i) Lines 1-2. Specifically, Menezes stated that this provides
7 uniqueness and timeliness assurances, and precludes certain replay and interleaving attacks. As
8 such, there is reasonable motivation to go against the preferred embodiment of not sending the
9 update data. Therefore, the examiner does not find the argument persuasive and has therefore
10 maintained the rejection presented in view of the combination of Fielder and Menezes.

11 Title

12 The title of the invention is acceptable.

13 Claim Rejections - 35 USC § 102

14 The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the
15 basis for the rejections under this section made in this Office action:

16 *A person shall be entitled to a patent unless –*

17 *(e) the invention was described in (1) an application for patent, published under section*
18 *122(b), by another filed in the United States before the invention by the applicant for patent or*
19 *(2) a patent granted on an application for patent by another filed in the United States before the*
20 *invention by the applicant for patent, except that an international application filed under the*
21 *treaty defined in section 351(a) shall have the effects for purposes of this subsection of an*
22 *application filed in the United States only if the international application designated the United*
23 *States and was published under Article 21(2) of such treaty in the English language.*

24
25 Claims 1, 5-8, and 16-19 are rejected under 35 U.S.C. 102(e) as being anticipated by
26 Fielder et al. (US Patent Number 5,995,624) hereinafter referred to as Fielder.

1 Regarding claim 1, Fielder disclosed a method for validating a client device (Originating
2 System) by a server device (Answering System) (See Fielder Abstract), said method comprising
3 the steps of: generating a shared unpredictable secret (See Fielder Col. 9 Paragraph 1 wherein the
4 unpredictable secret is the dynamic secret); storing the shared unpredictable secret client device
5 (See Fielder Col. 9 Lines 10-12) and in the server device (See Fielder Col. 10 Lines Paragraph
6 6); requiring the client device to prove that it holds a correct secret precondition to the server
7 device validating the client device (See Fielder Fig. 4b Steps 214-217 and Col. 10 paragraphs 4-
8 6); and replacing the shared unpredictable secret by a new shared unpredictable secret when the
9 server device validates the client device (See Fielder Col. 9 Lines 10-12 and Col. 10 paragraph
10 6).

11 Regarding claim 5, Fielder disclosed that the shared unpredictable secret is generated by
12 a generator from the group comprising a random number generator and a pseudo-random number
13 generator (See Fielder Col. 6 Paragraph 9).

14 Regarding claim 6, Fielder disclosed that the shared unpredictable secret comprises an
15 unpredictable component and a fixed component (See Fielder Col. 9 Lines 5-10 and Col. 6
16 Paragraph 9).

17 Regarding claim 7, Fielder disclosed that a plurality of devices desire to be validated by
18 the server device; and each client device has a unique unpredictable secret that it shares with the
19 server device (See Fielder Col. 13 Paragraphs 2-3).

20 Regarding claim 8, Fielder disclosed that following a validation of the client device, the
21 server device discards the original shared unpredictable secret and stores within server device a

Art Unit: 2131

1 new shared unpredictable secret that can be generated by applying update data to the original
2 shared unpredictable secret (See Fielder Col. 10 Paragraph 6 and Col. 6 paragraph 3).

3 Regarding claim 16, Fielder disclosed that the client device presents proof data to the server
4 device, wherein the proof data are derived from a shared unpredictable secret using a proof data
5 generation algorithm, and the proof data do not divulge the shared unpredictable secret (See
6 Fielder Col. 8 Lines 15-67); the server device checks the proof data by using a proof data
7 generation algorithm consistent with the proof data generation algorithm used by the client
8 device (See Fielder Col. 10 Lines 38-62); and when the server device determines that the proof
9 data presented by the client device were not generated from the same shared unpredictable secret
10 that is stored in both the client device and in the server device, the server device does not
11 validate the client device (See Fielder Col. 10 Lines 52-59).

12 Regarding claim 17, Fielder disclosed that each proof data generation algorithm is a one-
13 way function (See Fielder Col. 8 Lines 27-32, and Col. 10 Lines 16-27).

14 Regarding claim 18, Fielder disclosed a system for enabling a server device to validate a client
15 device, said system comprising: at least one client device (See Fielder Fig. 1 Element 10); a
16 server device (See Fielder Fig. 1 Element 11); a shared unpredictable secret (See Fielder Fig. 2
17 Element 21); means for storing the shared unpredictable secret the client device (See Fielder Fig.
18 1 Element 5b); means for storing the shared unpredictable secret the server device (See Fielder
19 Fig. 1 Element 17b); coupled to client device and to server device, means for determining
20 whether the client device holds a correct secret (See Fielder Fig. 3b Element 118 and Fig. 4b
21 Element 217); coupled to the determining means, means for allowing the server device to
22 validate the client device when the client device proves that it holds a correct secret (See Fig. 3b

Art Unit: 2131

1 Element 121 and Fig. 4b Elements 217-219); and coupled to the client device and to the server
2 device, means for replacing the original shared unpredictable secret with a new shared
3 unpredictable secret when server device validates the client device (See Fig. 3b Elements 123-
4 124 and Fig. 4b Elements 220-221) (Also see Fielder claims 1-19).

5 Regarding claim 19, Fielder disclosed a computer readable medium containing computer
6 program instructions for enabling a server device to validate client device (See Fielder Col. 5
7 Lines 63-65), said computer program instructions causing the execution of the following steps:
8 generating a shared unpredictable secret; storing the shared unpredictable secret in the client
9 device and in the server device; requiring the client device to prove that it holds a correct secret
10 as a precondition to allowing the client device to be validated by the server device; and replacing
11 the shared unpredictable secret by a new shared unpredictable secret when the client device is
12 validated by the server device (See the rejection of claim 1 above).

13 ***Claim Rejections - 35 USC § 103***

14 The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all
15 obviousness rejections set forth in this Office action:

16 *A patent may not be obtained though the invention is not identically disclosed or*
17 *described as set forth in section 102 of this title, if the differences between the subject matter*
18 *sought to be patented and the prior art are such that the subject matter as a whole would have*
19 *been obvious at the time the invention was made to a person having ordinary skill in the art to*
20 *which said subject matter pertains. Patentability shall not be negated by the manner in which*
21 *the invention was made.*
22

23 Claims 1, 5-8, 11-12, and 14-19 are rejected under 35 U.S.C. 103(a) as being
24 unpatentable over Fielder as applied to claim 1 above, and further in view of Menezes
25 (Handbook of Applied Cryptography).

1 Regarding claim 1, Fielder disclosed a method for validating a client device (Originating
2 System) by a server device (Answering System) (See Fielder Abstract), said method comprising
3 the steps of: generating a shared unpredictable secret (See Fielder Col. 9 Paragraph 1 wherein the
4 unpredictable secret is the dynamic secret); storing the shared unpredictable secret client device
5 (See Fielder Col. 9 Lines 10-12) and in the server device (See Fielder Col. 10 Lines Paragraph
6 6); requiring the client device to prove that it holds a correct secret precondition to the server
7 device validating the client device (See Fielder Fig. 4b Steps 214-217 and Col. 10 paragraphs 4-
8 6); and replacing the shared unpredictable secret by a new shared unpredictable secret when the
9 server device validates the client device (See Fielder Col. 9 Lines 10-12 and Col. 10 paragraph
10 6), and the originating system applying a random change value to the dynamic secret in order to
11 update the secret (See Fielder Col. 9 Paragraph 1), but failed to disclose the change value being
12 received from the answering system.

13 Menezes teaches a method for in which a verifier provides a challenge value to a
14 claimant, and the claimant applies the challenge to a known secret in which the time required to
15 respond to the challenge is monitored (See Menezes Pages 397-399 Especially Page 398 Section
16 (i) Random Numbers).

17 It would have been obvious to the ordinary person skilled in the art at the time of
18 invention to employ the teachings of Menezes in the authentication system of Fielder by having
19 the answering system create the random change value and provide it to the originating system.
20 This would have been obvious because the ordinary person skilled in the art would have been
21 motivated to protect against replay attacks, ensure timeliness of the reply, and therefore ensure

Art Unit: 2131

1 that the originator was in fact the holder of the dynamic secret, and further to lessen the
2 computation required of the originator, and token within.

3 Regarding claim 18, the combination of Fielder and Menezes disclosed a system for
4 enabling a server device to validate a client device, said system comprising: at least one client
5 device (See Fielder Fig. 1 Element 10); a server device (See Fielder Fig. 1 Element 11); a shared
6 unpredictable secret (See Fielder Fig. 2 Element 21); means for storing the shared unpredictable
7 secret the client device (See Fielder Fig. 1 Element 5b); means for storing the shared
8 unpredictable secret the server device (See Fielder Fig. 1 Element 17b); coupled to client device
9 and to server device, means for determining whether the client device holds a correct secret (See
10 Fielder Fig. 3b Element 118 and Fig. 4b Element 217); coupled to the determining means, means
11 for allowing the server device to validate the client device when the client device proves that it
12 holds a correct secret (See Fig. 3b Element 121 and Fig. 4b Elements 217-219); and coupled to
13 the client device and to the server device, means for replacing the original shared unpredictable
14 secret with a new shared unpredictable secret when server device validates the client device (See
15 Fig. 3b Elements 123-124 and Fig. 4b Elements 220-221) (Also see Fielder claims 1-19), said
16 means for replacing further comprising means for the server device to send update data to the
17 client device; means for the client device to apply the update data to the shared unpredictable
18 secret to generate a new secret; and means for the client device to replace the shared
19 unpredictable secret with the new secret (See the rejection of claim 1 above).

20 Regarding claim 19, the combination of Fielder and Menezes disclosed a computer
21 readable medium containing computer program instructions for enabling a server device to
22 validate client device (See Fielder Col. 5 Lines 63-65), said computer program instructions

1 causing the execution of the following steps: generating a shared unpredictable secret; storing the
2 shared unpredictable secret in the client device and in the server device; requiring the client
3 device to prove that it holds a correct secret as a precondition to allowing the client device to be
4 validated by the server device; and replacing the shared unpredictable secret by a new shared
5 unpredictable secret when the client device is validated by the server device, wherein the server
6 device sends update data to the client device; the client device applies the update data to the
7 shared unpredictable secret to generate a new secret; and the client device replaces the shared
8 unpredictable secret with the new secret (See the rejection of claim 1 above).

9 Regarding claim 5, the combination of Fielder and Menezes disclosed that the shared
10 unpredictable secret is generated by a generator from a group comprising a random number
11 generator and a pseudo-random number generator (See Fielder Col. 6 Paragraph 9).

12 Regarding claim 6, the combination of Fielder and Menezes disclosed that the shared
13 unpredictable secret comprises an unpredictable component and a fixed component (See Fielder
14 Col. 9 Lines 5-10 and Col. 6 Paragraph 9).

15 Regarding claim 7, the combination of Fielder and Menezes disclosed that a plurality of
16 devices desire to be validated by the server device; and each client device has a unique
17 unpredictable secret that it shares with the server device (See Fielder Col. 13 Paragraphs 2-3).

18 Regarding claim 8, the combination of Fielder and Menezes disclosed that following a
19 validation of the client device, the server device discards the shared unpredictable secret and
20 stores within server device the new shared unpredictable secret that can be generated by applying
21 the update data to the shared unpredictable secret (See Fielder Col. 10 Paragraph 6 and Col. 6
22 paragraph 3).

1 Regarding claim 11, the combination of Fielder and Menezes disclosed sending
2 acknowledgement data to the answering system to confirm that the originating system had
3 replaced the shared secret with the new secret (See Fielder Col. 8 Paragraphs 3-5).

4 Regarding claim 12, the combination of Fielder and Menezes disclosed the answering
5 system receiving the acknowledgement, validating the originating system, replacing the dynamic
6 secret with the new dynamic secret (See Fielder Col. 10 paragraph 5-6).

7 Regarding claims 14 and 15, the combination of Fielder and Menezes disclosed sending
8 proof data as acknowledgement data (See Fielder Col. 8 Paragraphs 3-4 wherein the dynamic
9 data was the new dynamic data from the previous session).

10 Regarding claim 16, the combination of Fielder and Menezes disclosed that the client
11 device presents proof data to the server device, wherein the proof data are derived from the
12 shared unpredictable secret using a proof data generation algorithm, and the proof data do not
13 divulge the shared unpredictable secret (See Fielder Col. 8 Lines 15-67); the server device
14 checks the proof data by using a proof data generation algorithm consistent with the proof data
15 generation algorithm used by the client device (See Fielder Col. 10 Lines 38-62); and when the
16 server device determines that the proof data presented by the client device were not generated
17 from the shared unpredictable secret that is stored in both the client device and in the server
18 device, the server device does not validate the client device (See Fielder Col. 10 Lines 52-59).

19 Regarding claim 17, the combination of Fielder and Menezes disclosed that each proof
20 data generation algorithm is a one-way function (See Fielder Col. 8 Lines 27-32, and Col. 10
21 Lines 16-27).

1
2
3 Claims 2-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fielder as
4 applied to claim 1 above, and further in view of Yatsukawa (US Patent Number 6,148,404).

5 Regarding claim 2, the combination of Fielder and Menezes disclosed both the
6 originating computer and the answering computer as containing the original dynamic secret (See
7 Fielder Col. 3 Paragraph 3), but failed to disclose how they both obtained the secret.

8 Yatsukawa teaches that in a one-time password system, a registration operation should be
9 performed in order to determine the initial secret (See Yatsukawa Col. 15 Line 65 – Col. 16 Line
10 12).

11 It would have been obvious to the ordinary person skilled in the art at the time of
12 invention to employ the teachings of Yatsukawa in the one-time password system of Fielder and
13 Menezes by having a registration step in which an initial secret was agreed upon and set in the
14 originating and answering systems. This would have been obvious because the ordinary person
15 skilled in the art would have been motivated to provide a means for both the systems to contain
16 identical secrets, as required by Fielder for the one-time password system to work properly.

17 Regarding claim 3, the combination of Fielder and Menezes and Yatsukawa disclosed
18 that a token can be activated by checking an activation code in order to use the system (See
19 Fielder Col. 13 Paragraph 2), and also checking a user id and email address and other such
20 information (See Yatsukawa Col. 16 Paragraph 2).

21 Regarding claim 4, the combination of Fielder and Menezes and Yatsukawa disclosed
22 that the token must be purchased (See Fielder Col. 12 Lines 64-67).

Claims 10, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Fielder and Menezes as applied to claim 1 above, and further in view of Lamport, Leslie (Password Authentication with Insecure Communication).

Fielder and Menezes disclosed the change value being random and applying the change value to the dynamic secret to create a new dynamic secret (See Fielder Col. 6 Paragraph 9), and providing proof data that the originating system held the correct dynamic secret (See Fielder Col. 8 Paragraph 5), however, failed to disclose that the applying was a one-way function, and also failed to disclose that proof of any future dynamic password would suffice.

Lamport teaches a method for applying updates to a secret and verifying knowledge of the secret in which the update applied is a one-way function, and in which knowledge of any future proof, can be used to grant authentication (See Lamport Section II).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Lamport in the authentication system of Fielder and Menezes by using a one-way function to update the dynamic secret and further by allowing knowledge of any future password to grant authentication. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow a simple means for re-synchronizing the dynamic secrets held in the originating device and the answering device while protecting against replay attacks.

Conclusion

Claims 1-8, and 10-19 have been rejected and claim 9 has been cancelled.

Art Unit: 2131

1 **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time
2 policy as set forth in 37 CFR 1.136(a).

3 A shortened statutory period for reply to this final action is set to expire **THREE**
4 **MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO**
5 **MONTHS** of the mailing date of this final action and the advisory action is not mailed until after
6 the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period
7 will expire on the date the advisory action is mailed, and any extension fee pursuant to 37
8 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,
9 however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing
10 date of this final action.

11 Any inquiry concerning this communication or earlier communications from the
12 examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790.
13 The examiner can normally be reached on M-F 8-4.

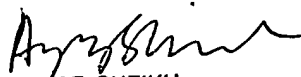
14 If attempts to reach the examiner by telephone are unsuccessful, the examiner's
15 supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the
16 organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

1 Information regarding the status of an application may be obtained from the Patent
2 Application Information Retrieval (PAIR) system. Status information for published applications
3 may be obtained from either Private PAIR or Public PAIR. Status information for unpublished
4 applications is available through Private PAIR only. For more information about the PAIR
5 system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR
6 system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

7
8
9
10 

11 Matthew Henning
12 Assistant Examiner
13 Art Unit 2131
14 7/21/2005


11 AYAZ SHEIKH
12 SUPERVISORY PATENT EXAMINER
13 TECHNOLOGY CENTER 2100